На правах рукописи

Ключарёв Петр Георгиевич

Высокопроизводительные алгоритмы специальной обработки данных для защиты компьютерных сетей, ориентированные на аппаратную реализацию

05.13.15 – Вычислительные машины, комплексы и компьютерные сети

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
доктора технических наук

Москва – 2022

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)».

Официальные оппоненты:

Шелухин Олег Иванович,
доктор технических наук, профессор, заслуженный деятель науки РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики», заведующий кафедрой «Информационная безопасность»

Сельвесюк Николай Иванович,
доктор технических наук, доцент, профессор РАН
Федеральное автономное учреждение «Государственный научно-исследовательский институт авиационных систем», заместитель генерального директора — руководитель научного комплекса

Дворянкин Сергей Владимирович,
доктор технических наук, профессор
Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина», профессор кафедры комплексной безопасности критически важных объектов

Ведущая организация:

Федеральное государственное бюджетное учреждение «Национальный исследовательский центр «Курчатовский институт»

Защита состоится 29 сентября 2022 г. в 13:00 на заседании диссертационного совета Д 999.216.02 при МАИ и МГТУ им. Н. Э. Баумана по адресу: 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1, зал Ученого совета ГУК.

С диссертацией можно ознакомиться в библиотеке МГТУ им. Н.Э. Баумана и на сайте http://bmstu.ru.

Отзыв на автореферат в двух экземплярах, заверенных печатью организации, просим направлять по адресу: 105005, г. Москва, 2-я Бауманская ул., д. 5, стр. 1, ученому секретарю диссертационного совета Д 999.216.02.

Автореферат разослан «____» _____ 2022 г.

Ученый секретарь
диссертационного совета Д 999.216.02
доктор технических наук, доцент А. Н. Алфимцев

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. В настоящее время скорости передачи информации в компьютерных сетях быстро возрастают. Так, в 2017 г. стандартизованы протоколы для организации компьютерных сетей, функционирующих на скоростях до 400 Гбит/с (стандарт IEEE 802.3bs–2017). Уже производится поддерживающее этот стандарт оборудование. В ближайшие годы ожидается стандартизация более высокоскоростных протоколов. При этом современные компьютерные сети должны быть хорошо защищены от угроз нарушения конфиденциальности и целостности передаваемых в них данных. Для этого применяется целый ряд методов, среди которых одними из важнейших являются алгоритмические.

Основным видом алгоритмов специальной обработки данных для защиты компьютерных сетей от угроз нарушения конфиденциальности и целостности обрабатываемой в них информации являются криптографические алгоритмы, среди которых огромное значение имеют симметричные криптографические алгоритмы, такие как алгоритмы поточного шифрования, алгоритмы блочного шифрования, криптографические хэш-функции, алгоритмы выработки имитовставки. В настоящее время известно довольно большое число таких алгоритмов. Среди них есть как универсальные, так и ориентированные либо на программную, либо на аппаратную реализацию. Такие алгоритмы разрабатывались многими учеными, среди которых Д. Бернштайн, А. Бирюков, Э. Бихам, Й. Даймен, Л. Кнудсен, Р. Меркль, Дж. Мэсси, Б. Пренель, Р. Ривест, В. Рэймен, Н. Фергюсон, Х. Фейстель, Б. Шнайер и др.

Криптографические алгоритмы могут обладать значительной вычислительной сложностью, фактически ограничивая пропускную способность защищенных компьютерных сетей. Поэтому для защиты современных и перспективных высокопроизводительных компьютерных сетей требуются новые криптоалгоритмы, обладающие высокой скоростью работы. Кроме того, в настоящее время активно развиваются сети «умных» устройств, обладающих ограниченными вычислительными ресурсами, однако ведущих обмен информацией с высокой скоростью. К ним относятся множество различных сетей: от интернета вещей (Internet of things), до тактических сетей различного назначения (в рамках концепции сетецентрической войны). К защищенности таких сетей предъявляются высокие требования, что обуславливает необходимость применения стойких криптографических алгоритмов, которые могут быть реализованы в условиях ограниченных вычислительных ресурсов. Такие криптоалгоритмы часто называют низкоресурсными, а направление криптографии, занимающееся разработкой таких криптоалгоритмов, называется низкоресурсной (легковесной, lightweight) криптографией.

Таким образом, несмотря на существование достаточно большого количества симметричных криптографических алгоритмов, разработка новых криптоалгоритмов, как ориентированных на достижение высокой производительности при аппаратной реализации, так и предназначенных для низ-

коресурсных аппаратных реализаций, в настоящее время весьма актуальна. Анализ литературы показал, что весьма перспективным является использование в качестве основы таких алгоритмов обобщённых клеточных автоматов (ОКлА). ОКлА являются обобщением классических клеточных автоматов, впервые предложенных Дж. фон Нейманом и широко исследованных разными авторами, среди которых С. Вольфрам, Дж. Конвей, В.Б. Кудрявцев, Э. Мур, Н. Марголус, Т. Тоффоли, С. Улам и многие другие. Основные исследования в области свойств клеточных автоматов, применительно к задачам криптографии и генерации псевдослучайных последовательностей принадлежат С. Вольфраму. Применением клеточных автоматов для генерации псевдослучайных последовательностей занимались ряд авторов, среди которых особо отметим Б.М. Сухинина, впервые предложившего использовать обобщение клеточного автомата для построения высокоскоростного генератора псевдослучайных последовательностей, предназначенного для аппаратной реализации. Высокая производительность и низкие требования к аппаратным ресурсам этого генератора позволяют предположить, что на основе ОКлА можно производить построение как высокопроизводительных, так и низкоресурсных алгоритмов симметричного шифрования, ориентированных на аппаратную реализацию. Именно этой весьма актуальной теме и посвящена диссертация.

Цели и задачи диссертационной работы. Целью диссертационной работы является повышение пропускной способности компьютерных сетей, при условии обеспечения их защищенности от угроз нарушения конфиденциальности и целостности передаваемых в них данных.

Для достижения поставленной цели в диссертационной работе решены следующие задачи:

1. Разработка методов синтеза ОКлА, предназначенных для построения на их основе криптографических алгоритмов, ориентированных на аппаратную реализацию. В том числе исследование методов построения графов таких ОКлА и построение локальных функций связи.
2. Разработка метода построения псевдослучайных функций-кандидатов на основе ОКлА, предназначенных для использования в составе криптографических алгоритмов, ориентированных на аппаратную реализацию.
3. Разработка семейств алгоритмов блочного шифрования, алгоритмов поточного шифрования, криптографических хэш-функций и алгоритмов выработки имитовставки, основанных на ОКлА и ориентированных на аппаратную реализацию.
4. Статистическое тестирование разработанных псевдослучайных функций-кандидатов и криптографических алгоритмов.
5. Исследование криптостойкости разработанных криптоалгоритмов;
6. Реализация разработанных криптографических алгоритмов на программируемых логических интегральных схемах. Тестирование производительности.

Научная новизна.

1. Разработаны теоретические положения (в том числе сформулированы и доказаны теоремы), позволяющие производить синтез ОКлА, предназначенных для построения на их основе симметричных криптографических алгоритмов, ориентированных на аппаратную реализацию. В том числе предложены научно-обоснованные требования к графам и локальным функциям связи таких ОКлА, построено семейство удовлетворяющих им локальных функций связи и выбраны способы построения удовлетворяющих им графов. Впервые предложено использовать графы Рамануджана в качестве графов таких ОКлА.
2. Разработан метод построения псевдослучайных функций-кандидатов, основанных на ОКлА, графами которых являются графы Рамануджана. Эти функции применяются для построения симметричных криптоалгоритмов, ориентированных на аппаратную реализацию.
3. Построено семейство алгоритмов поточного шифрования, основанных на ОКлА, графами которых являются графы Рамануджана. В этом семействе существуют алгоритмы, аппаратные реализации которых показывают производительность в 50 раз более высокую, чем производительность аппаратных реализаций лучших аналогов.
4. Построено семейство алгоритмов блочного шифрования, основанных на ОКлА. Алгоритмы из этого семейства при аппаратной реализации показывают высокую производительность, а также низкие требования к аппаратным ресурсам.
5. Построены два семейства криптографических хэш-функций, основанных на ОКлА, и семейство алгоритмов выработки имитовставки, основанных на ОКлА. Хэш-функции из этих семейств при аппаратной реализации показывают высокую производительность, а также низкие требования к аппаратным ресурсам.
6. Исследована стойкость криптографических алгоритмов, основанных на ОКлА, по отношению к линейному, алгебраическому, логическому, разностному и квантовому методам криптоанализа. Проведено статистическое тестирование построенных алгоритмов. Доказана NP-трудность задачи восстановления предыдущего состояния ОКлА.

Теоретическая значимость. В диссертации предложен комплекс научных результатов, который можно рассматривать как методологию синтеза симметричных криптоалгоритмов, основанных на ОКлА. Эта методология позволяет разрабатывать алгоритмы поточного шифрования, алгоритмы блочного шифрования, криптографические хэш-функции и алгоритмы выработки имитовставки, ориентированные на высокопроизводительную аппаратную реализацию и предназначенные для использования в составе аппаратных средств защиты компьютерных сетей от угроз нарушения конфиденциальности и целостности обрабатываемых в них данных.

Практическая ценность. В работе продемонстрировано, что производительность построенных криптографических алгоритмов при реализации на программируемых логических интегральных схемах (ПЛИС) значительно превышает производительность существующих криптографических алгоритмов. Использование построенных криптоалгоритмов позволяет повысить пропускную способность защищенных компьютерных сетей. Кроме того, построенные криптоалгоритмы допускают низкоресурсную реализацию, что позволяет использовать их на различных аппаратных вычислительных устройствах, обладающих ограниченными вычислительными ресурсами. Также построенные криптоалгоритмы могут быть с достаточной эффективностью реализованы на графических процессорах.

В ходе работы над диссертацией разработан большой объем вспомогательного ПО.

Методы исследования. Использовались методы теории графов (в том числе алгебраической и спектральной), теории алгоритмов, теории булевых функций, математической статистики, криптографии, криптоанализа, теории групп, теории колец.

Для разработки ПО использовались языки программирования C++, Python (при этом использовались разнообразные библиотеки, в частности, NetworkX, NZMath и др.), C# и R. Кроме того, использовались системы компьютерной алгебры Magma и Wolfram Mathematica. В качестве языка описания архитектуры ПЛИС использовался VHDL.

На защиту выносится:

1. Теоретические положения и доказанные теоремы, позволяющие производить построение ОКлА, предназначенных для применения в качестве основы высокопроизводительных симметричных криптографических алгоритмов, ориентированных на аппаратную реализацию.
2. Метод построения псевдослучайных функций-кандидатов, основанных на ОКлА и предназначенных для использования в составе криптографических алгоритмов, ориентированных на аппаратную реализацию.
3. Семейство ориентированных на аппаратную реализацию высокопроизводительных алгоритмов поточного шифрования, основанных на ОКлА.
4. Семейство ориентированных на аппаратную реализацию высокопроизводительных алгоритмов блочного шифрования, основанных на ОКлА.
5. Семейства ориентированных на аппаратную реализацию высокопроизводительных криптографических хэш-функций и алгоритмов выработки имитовставки, основанных на ОКлА.
6. Результаты статистического тестирования построенных псевдослучайных функций-кандидатов и разработанных семейств криптоалгоритмов, показывающие их высокое статистическое качество.
7. Результаты исследования стойкости криптографических алгоритмов, основанных на ОКлА, показывающие высокий уровень их криптостойкости.

Достоверность результатов работы подтверждается корректным применением математического аппарата, совокупностью доказанных теорем, а также результатами проведенных вычислительных экспериментов.

Соответствие специальности. Диссертация посвящена разработке ориентированных на аппаратную реализацию алгоритмов специальной обработки данных, в том числе алгоритмов поточного шифрования, алгоритмов блочного шифрования, криптографических хэш-функций и алгоритмов выработки имитовставки, что обуславливает соответствие п. 3 паспорта специальности. Такие алгоритмы повсеместно применяются для защиты компьютерных сетей, что обуславливает соответствие п. 5 паспорта специальности. При этом, криптографические хэш-функции широко используются в задачах обеспечения надежности и организации контроля передачи данных в компьютерных сетях, что обуславливает соответствие п. 6 паспорта специальности. Кроме того, ОКлА, на которых основаны разрабатываемые в диссертации алгоритмы, обеспечивают высокую степень параллельности обработки информации, что обуславливает соответствие п. 4 паспорта специальности.

Апробация результатов. Результаты диссертации докладывались на Второй, Третьей, Четвертой, Седьмой, Восьмой, Девятой всероссийских научных конференциях «Безопасные информационные технологии» (г. Москва, 2011, 2012, 2013, 2016, 2017, 2018 гг.); Десятой и Одиннадцатой международных научных конференциях «Безопасные информационные технологии» (г. Москва, 2019, 2021 гг.); Межвузовской научной конференции «Инновационные методы обучения в заочной системе образования» (г. Москва, 2013 г.); Одиннадцатой международной научно-практической конференции «Перспективы развития информационных технологий» (г. Новосибирск, 2013 г.); Междисциплинарном научном семинаре «Экобионика» (г. Москва, 2019 г.).

Работа выполнялась при поддержке грантов РФФИ 12-07-31012 мол_а (2012–2013 гг., руководитель), 16-07-00542 а (2016–2018 гг., руководитель), 20-17-50258 (2020 г., руководитель), 16-29-09517 офи-м (2016–2017 гг.).

В 2013 г. проект, посвященный использованию обобщенных клеточных автоматов в криптографии, выполняемый под руководством автора, вышел в финал Первого Всероссийского конкурса научно-исследовательских работ среди граждан РФ в интересах Вооруженных сил РФ и отмечен Грамотой Министерства обороны РФ.

Внедрение. Результаты диссертации внедрены в научно-производственную деятельность ПАО РКК Энергия им. С.П. Королёва, АО «НПО Эшелон» и ООО «Алгоритмы и данные», а также в учебный процесс МГТУ им. Н.Э. Баумана.

Публикации. По теме диссертации автором опубликовано 43 работы, из них 28 — в журналах, входящих в перечень ВАК РФ.

Личный вклад автора. Все представленные в диссертации научные результаты получены лично автором.

Структура и объем диссертации. Диссертация состоит из введения,

шести глав, заключения и списка литературы. Полный объем диссертации — 297 страниц, включая 63 рисунка и 32 таблицы. Список литературы состоит из 439 источников.

СОДЕРЖАНИЕ РАБОТЫ

Во введении кратко обоснована актуальность диссертационной работы, поставлены цель и задачи, сформулирована научная новизна и показана практическая значимость полученных результатов, представлены выносимые на защиту научные результаты, приведены сведения об апробации и внедрении результатов диссертации.

В первой главе произведен краткий обзор современного состояния предметной области. Кратко рассматриваются современные проблемы, связанные с защитой высокоскоростных компьютерных сетей. Рассматриваются современные алгоритмы поточного шифрования, блочного шифрования и криптографические хэш-функции. Кратко обсуждается проблематика, связанная с низкоресурсной (lightweight) криптографией.

Кратко рассмотрены некоторые факты из теории клеточных автоматов в контексте ее применения в криптографии. *Классический клеточный автомат* — это упорядоченный набор ячеек памяти, которые образуют d-мерную решетку. В каждой ячейке может храниться значение, принадлежащее некоторому конечному множеству (в большинстве случаев — $\mathbb{Z}_2$). Автомат работает по шагам. Значения всех ячеек изменяются одновременно на каждом шаге, в соответствии с некоторыми правилами перехода. При этом значение ячейки памяти на очередном шаге зависит только от значений ячеек, принадлежащих некоторой ее окрестности на предыдущем шаге, правила перехода являются одинаковыми для всех ячеек решетки клеточного автомата, а противоположные края решетки обычно отождествляются. Понятие клеточного автомата было предложено Дж. фон Нейманом в 1951 г. в качестве модели самоорганизующихся систем.

Далее рассматриваются обобщенные клеточные автоматы, дается определение этого понятия и кратко обсуждается история его возникновения. Назовем *обобщённым клеточным автоматом* (*ОКлА*) ориентированный граф (*граф ОКлА*) с множеством вершин $V = \{v_1, \ldots, v_N\}$, с каждой вершиной v_i которого ассоциированы

- булева переменная m_i, которая называется *ячейкой*;
- булева функция $f_i(x_1, \ldots, x_{d_i})$, которая называется *локальной функцией связи* (*ЛФС*) вершины v_i (d_i — степень захода вершины v_i).

При этом каждой паре (v, e), где $v \in V$ — вершина, e — входящее в неё ребро, соответствует номер аргумента ЛФС, вычисляемой в вершине v. Будем называть его *номером ребра e относительно вершины v*. Отметим, что здесь и далее мы используем термин «граф», допуская наличие петель и кратных рёбер.

Опишем теперь работу ОКлА. В начальный момент времени каждая

ячейка m_i, $i \in \{1, 2, ..., N\}$, имеет некоторое начальное значение $m_i(0)$. ОКлА работает пошагово. Значения ячеек на шаге t вычисляются по формуле:

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)), \qquad (1)$$

где $\eta(i, j)$ – номер вершины, из которой выходит ребро, входящее в вершину v_i и имеющее относительно этой вершины номер j.

Заполнением (*состоянием*) ОКлА на шаге t будем называть набор значений ячеек $M(t) = (m_1(t), m_2(t), \ldots, m_N(t))$. *Размером* ОКлА будем называть число ячеек. ОКлА будем называть *однородным*, если для любого $i \in \{1, ..., N\}$ выполняется $f_i = f$, то есть ЛФС для всех ячеек одинакова. Степени захода вершин графа такого ОКлА, очевидно, одинаковы: $d_1 = d_2 = \ldots = d_N = d$. Назовем ОКлА *неориентированным*, если для любого ребра (u, v) в его графе существует и ребро (v, u). Граф такого ОКлА можно рассматривать как неориентированный, для чего достаточно заменить каждую пару ориентированных рёбер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$. В данной работе мы будем в основном рассматривать неориентированные однородные ОКлА. Такой ОКлА задается тройкой (G, f, η), где G — d-регулярный граф ОКлА (множество его вершин $V = \{v_1, \ldots, v_N\}$), а $\eta : \{1, \ldots, N\} \times \{1, \ldots, d\} \to \{1, \ldots, N\}$ — введенная выше функция (будем называть ее функцией нумерации ребер).

Некоторый набор ячеек ОКлА будем называть *выходом*. Последовательность значений выходов будем называть *выходной последовательностью*. *Последовательностью заполнений* ОКлА A назовем функцию $F_A : \{0, 1\}^N \times \mathbb{N} \to \{0, 1\}^N$, аргументами которой является начальное заполнение ОКлА и номер шага, а значением — заполнение ОКлА на этом шаге. *Периодом ОКлА* будем называть период его выходной последовательности.

Фактически, ОКлА представляет собой автономный конечный автомат и является обобщением классического клеточного автомата. Подобные обобщения под разными названиями использовались в различных областях. По-видимому, впервые подобное понятие появилось в 1969 г. в работе С. Кауфмана, где оно использовалось в области биологии. После этого, в исследовании подобных моделей наступил перерыв, который закончился лишь после 2000 года, когда появился ряд работ, в которых исследовались модели, в той или иной степени аналогичные определенному выше ОКлА. Называли их в этих статьях по-разному, например, булевыми сетями (Boolean networks), сетями Кауфмана, графовыми клеточными автоматами и др. При этом отношение к таким моделям как к обобщению клеточных автоматов более характерно для российской научной школы. Развитие такие модели получили в 2009–2011 гг. в работах Б.М. Сухинина, который предложил использовать аналогичную модель для генерации псевдослучайных последовательностей на аппаратных платформах.

Проведенный обзор литературы дал основание выдвинуть гипотезу, что на основе ОКлА можно создать высокопроизводительные симметричные

криптографические алгоритмы, предназначенные для аппаратной реализации. Исходя из этого произведена постановка цели и задач диссертации.

Вторая глава посвящена вопросам построения ОКлА, предназначенных для применения в задачах построения симметричных криптоалгоритмов, ориентированных на аппаратную реализацию.

Введем некоторые определения. Пусть задана двоичная последовательность $\{\xi_t\}$. Назовем *ОКлА с задающей последовательностью* ОКлА, у которого для вычисления значений одной из ячеек m_r, для некоторого $r \in \{1, \ldots, N\}$ (будем называть эту ячейку *задающей ячейкой*), вместо формулы (1) используется формула:

$$m_r(t) = f_r\left(m_{\eta(r,1)}(t-1), m_{\eta(r,2)}(t-1), \ldots, m_{\eta(r,d_r)}(t-1)\right) \oplus \xi_t. \qquad (2)$$

Построение ЛФС. В диссертации обоснованы следующие требования к ЛФС: ЛФС должна быть равновесной, шефферовой и как можно более нелинейной, но линейно зависящей от одного из своих аргументов. Кроме того, при применении ОКлА в составе алгоритма поточного шифрования, должна обеспечиваться нижняя оценка периода выходной последовательности. *Нелинейность* булевой функции g, т.е. расстояние Хемминга от этой функции до множества аффинных булевых функций, будем обозначать $\Lambda(g)$.

Будем говорить, что ОКлА вычисляет булеву функцию $\varphi(x_1, \ldots, x_n)$, если существуют такие $j_0 \in \{1, \ldots, N\}$, $t_0 \in \mathbb{Z}^+$ и набор $(j_1, \ldots, j_n) \in \{1, \ldots, N\}^n$, элементы которого попарно различны, что выполняется $m_{j_0}(t_0) = \varphi(m_{j_1}(0), \ldots, m_{j_n}(0))$. В диссертации доказана следующая теорема, показывающая полноту ОКлА, как вычислительной модели, и устанавливающая связь между ОКлА и булевыми схемами.

Теорема 1. *Булеву функцию $\varphi(x_1, \ldots, x_n)$, имеющую при реализации булевой схемой над базисом B сложность l и глубину h, можно вычислить с помощью ОКлА, ЛФС которого принадлежат B, а граф имеет $n + l$ вершин, причем для этого требуется не более h шагов.*

Фактически, ОКлА можно рассматривать как вычислительную модель параллельной обработки информации. В диссертации показано, что такая модель позволяет создавать специальные алгоритмы, обладающие высокой производительностью при аппаратной реализации.

В диссертации подробно исследован вопрос о построении семейства ЛФС, удовлетворяющих приведенным выше требованиям. Построение этого семейства производится на основе бент-функций, для синтеза которых используется метод Ротхауса, состоящий в том, что бент-функция строится в виде: $\beta(x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s(x_1, \ldots, x_k)$, где $s(x_1, \ldots, x_k)$ — произвольная булева функция.

Построены функции вида:

$$g_1(u, x_1, y_1, \ldots, x_k, y_k) = \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus u, \qquad (3)$$

$$g_2(v, u, x_1, y_1, \ldots, x_k, y_k) =$$
$$= \bigoplus_{i=1}^{k} x_i y_i \oplus s_1(x_1, \ldots, x_k) \oplus v(s_1(x_1, \ldots, x_k) \oplus s_3(x_1, \ldots, x_k)) \oplus u, \quad (4)$$

где s_1 и s_3 — булевы функции, о выборе которых написано ниже.

В диссертации доказано, что функции, заданные формулами (3) и (4) удовлетворяют всем приведенным выше требованиям и могут использоваться в качестве ЛФС. При этом, в случае нечетного числа переменных используются функции, заданные формулой (3). В этой формуле $s_1(x_1, \ldots, x_k)$ — произвольная булева функция, для которой выполняется $k + t_1 = 1 \pmod 2$, где t_1 — число ненулевых коэффициентов в АНФ функции s_1 и, при этом, свободный член АНФ функции s_1 равен 1. В случае четного числа переменных используются функции, заданные формулой (4). В этой формуле $s_1(x_1, \ldots, x_k)$ и $s_3(x_1, \ldots, x_k)$ — произвольные булевы функции, для которых выполняется $k + t_3 = 1 \pmod 2$, где t_3 — число ненулевых коэффициентов в АНФ функции s_3 и, при этом, свободный член АНФ функции s_1 равен 1.

Нелинейности функций g_1 и g_2, заданных формулами (3), (4), имеют следующие нижние оценки, близкие к максимально возможным:

$$\Lambda(g_1) \geqslant 2^{2k} - 2^k; \Lambda(g_2) \geqslant 2^{2k+1} - 2^{k+1}. \quad (5)$$

Приведем пример ЛФС из построенного семейства:

$$f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1x_3x_5 \oplus x_3x_4 \oplus x_5x_6 \oplus x_3x_5 \oplus x_1x_5 \oplus x_1 \oplus x_2 \oplus 1. \quad (6)$$

Далее в диссертации рассмотрены вопросы обеспечения нижней оценки периода. Доказаны теоремы, позволяющие выбрать задающую ячейку ОКлА с задающей последовательностью таким образом, чтобы период его выходной последовательности был не меньшим, чем период задающей последовательности. Для того, чтобы это было возможно, требуется, чтобы ЛФС была линейной относительно одного из своих аргументов. Породить задающую последовательность можно с помощью любого генератора псевдослучайных последовательностей, для которого известна нижняя оценка периода, например — линейного регистра сдвига с обратной связью (LFSR), характеристический многочлен которого является примитивным.

Построение графов ОКлА. Криптографические свойства ОКлА во многом определяются его графом. Рассмотрим сначала характеристики лавинного эффекта ОКлА. Лавинный эффект заключается в способности дискретной динамической системы существенно изменять выходную последовательность при небольших изменениях входных данных.

Ранее Б.М. Сухининым была введена интегральная характеристика лавинного эффекта: $\omega(t) = \frac{1}{N} \sum_{j=1}^{N} \left(m_j^{(1)}(t) \oplus m_j^{(2)}(t) \right)$. Здесь $(m_1^{(1)}, ..., m_N^{(1)})$ и $(m_1^{(2)}, ..., m_N^{(2)})$ — наборы ячеек двух идентичных неориентированных ОКлА, начальное заполнение которых отличается только в одной ячейке (для определенности — m_1).

Введем *пространственную характеристику лавинного эффекта ОКлА*:

$$\mu(t) = \frac{1}{e(1)} \cdot \max_{j \in \{1,2,\ldots,N\}} \left(\left(m_j^{(1)}(t) \oplus m_j^{(2)}(t) \right) \cdot \Delta(1,j) \right), \qquad (7)$$

где $\Delta(i,j)$ — расстояние между i-й и j-й вершинами графа ОКлА, а $e(i)$ — эксцентриситет i-й вершины.

Рассмотрим усредненные по большому количеству начальных заполнений интегральную и пространственную характеристики лавинного эффекта: $\hat{\omega}(t)$ и $\hat{\mu}(t)$. Начиная с некоторого t_n, для некоторых наперед заданных констант ε_1 и ε_2 выполняется $|\hat{\omega}(t) - \omega_n| \le \varepsilon_1$ и $|\hat{\mu}(t) - \mu_n| \le \varepsilon_2$ при $t \ge t_n$. Для обеспечения хороших статистических свойств выходной последовательности необходимо, чтобы $\omega_n = 0.5$, а $\mu_n = 1$.

Исходя из изложенного, а также из ряда других соображений, в диссертации обосновывается следующий набор требований к графу однородного неориентированного ОКлА:

- граф должен иметь свойства, близкие к свойствам случайного графа;
- диаметр графа должен быть как можно меньшим;
- граф должен быть регулярным;
- граф не должен быть двудольным;
- граф должен иметь как можно меньшее число петель и кратных ребер;
- граф должен иметь как можно меньшую степень;
- степень графа должна быть не меньше четырех;
- в семействе графов должно существовать достаточно много графов с числом вершин от нескольких десятков до нескольких тысяч.

Этим требованиям удовлетворяют расширяющие графы, в особенности, так называемые графы Рамануджана.

Как известно, *коэффициентом рёберного расширения* неориентированного d-регулярного графа G с множеством вершин V называется величина $h(G) = \min\limits_{S \subset V : 0 < |S| \le \frac{|V|}{2}} \frac{|\partial S|}{|S|}$, где $|\partial S|$ — число рёбер, каждое из которых соединяет вершину из множества S с вершиной из множества $V \setminus S$. *Расширяющим графом* (expander graph) называется неориентированный регулярный граф G, для которого $h(G) \ge c$, где c — некоторая наперёд заданная положительная константа. Коэффициент рёберного расширения графа связан с его спектром. Спектр неориентированного графа — это набор собственных значений его матрицы смежности, отсортированный по невозрастанию: $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_N$. Здесь и далее N — число вершин графа. Как известно из спектральной теории графов, для d-регулярных графов $\lambda_1 = d$ и справедливо следующее *неравенство Чигера*: $\frac{1}{2}(d - \lambda_2) \le h(G) \le \sqrt{2d(d - \lambda_2)}$. Введем обозначение: $\lambda = \lambda(G) = \max_{|\lambda_i| < d} |\lambda_i|$.

Для диаметра расширяющего графа известно неравенство: $D \leqslant \left\lceil \log_{d/|\lambda_2|} (N-1) \right\rceil$. Из этого следует, что хорошими графами неориентированных ОКлА могут являться графы с маленьким значением параметра λ_2. В качестве таких графов будем использовать графы Рамануджана,

которые можно рассматривать как в определенном смысле наилучшие расширяющие графы. *Графом Рамануджана* называется связный d-регулярный неориентированный граф G, для которого справедливо неравенство:

$$\lambda(G) \leq 2\sqrt{d-1}. \tag{8}$$

Для диаметра $D(G)$ графов Рамануджана известно соотношение: $D(G) \leq 2\log_{d-1} N + \mathrm{O}(1)$. Эта верхняя оценка диаметра графа Рамануджана близка к нижней оценке диаметра регулярного графа. Можно обоснованно предположить, что использование графов Рамануджана в качестве графов ОКлА, предназначенных для криптографических применений, позволяет обеспечить хорошие характеристики лавинного эффекта.

Известны следующие подходы к построению небольших графов Рамануджана: построение при помощи известного детерминированного метода и случайная генерация с последующей проверкой значения λ.

Известно, что случайный регулярный граф с большой вероятностью является графом Рамануджана. Поэтому генерировать графы Рамануджана можно с помощью следующего алгоритма, основанного на случайном выборе регулярного графа:

1. Сгенерировать случайный регулярный граф G с заданным числом вершин (для этого известен алгоритм, обладающий вычислительной сложностью $O(Nd^2)$).
2. Проверить граф G на связность. Если он не связен, перейти к п. 1.
3. Вычислить $\lambda(G)$. Если условие (8) не выполняется, то перейти к п. 1.

Для параметров случайных регулярных графов известны различные асимптотические оценки, однако для практических целей важно более точно знать какие значения могут принимать параметры для небольших графов малой степени. С целью установления этого проведен вычислительный эксперимент. Автором разработано ПО, с помощью которого сгенерировано большое число (около 450 тыс.) небольших случайных регулярных графов. Для всех них были вычислены значения λ. Плотности распределений этих значений, а также распределения значений диаметров графов, приведены в диссертации. Результаты вычислительного эксперимента показали, что графы Рамануджана появляются с большой вероятностью, а диаметры полученных графов весьма малы. Вычисления заняли около шести суток на компьютере с 16-ю ядрами Intel Xeon E5-2690 и 16 ГБ ОЗУ.

Далее в главе рассматриваются известные детерминированные методы построения графов Рамануджана с тем, чтобы выбрать подходящие. Рассматриваются следующие семейства графов Рамануджана: семейство $X^{p,q}$ Любоцкого–Филипса–Сарнака (LPS-X), семейство $Y^{p,q}$ Любоцкого–Филипса–Сарнака (LPS-Y), семейство графов Моргенштерна и семейство графов Пайзера. В диссертации устанавливается, что для использования в качестве графов ОКлА подходят графы LPS-Y и графы Пайзера.

Кратко рассмотрим семейство LPS-Y. Графы, ему принадлежащие, яв-

ляются недвудольными. Опишем метод их построения. Выберем простые числа p и q, для которых выполняются условия: $p \equiv 1 \pmod 4; q \equiv 1 \pmod 4; p \neq q; \left(\frac{p}{q}\right) = 1$, где $\left(\frac{p}{q}\right)$ — символ Лежандра. Множеством V вершин графа $Y^{p,q}$ является проективная прямая над конечным полем $\mathbb{F}_q$, т.е., $V = \mathbb{F}_q \cup \{\infty\}$. Каждая вершина $u \in V$ соединена ребром с вершиной v:

$$v = \begin{cases} \frac{(a_0+ia_1)u+(a_2+ia_3)}{(-a_2+ia_3)u+(a_0-ia_1)}, & \text{если } (a_2 - ia_3)u \neq a_0 - ia_1 \text{ и } u \neq \infty, \\ \infty, & \text{если } (a_2 - ia_3)u = a_0 - ia_1 \text{ и } u \neq \infty, \\ \frac{ia_1+a_0}{ia_3-a_2}, & \text{если } ia_3 \neq a_2 \text{ и } u = \infty, \\ \infty, & \text{если } ia_3 = a_2 \text{ и } u = \infty, \end{cases} \tag{9}$$

для каждой четверки $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, такой, что a_0 — нечетное положительное, a_1, a_2, a_3 — четные и выполняется равенство: $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. Здесь $i \in \mathbb{F}_q$ такое, что $i^2 + 1 = 0$. Граф имеет степень $p + 1$.

Различных графов из семейства $Y^{p,q}$ с числом вершин от 100 до 10000 для $p = 5$ (т.е. 6-регулярных) насчитывается 298, а для $p = 13$ (т.е. 14-регулярных) — 301. В целях проведения вычислительных экспериментов автором разработано ПО, с помощью которого было построено 448 таких графов степени 6 с числом вершин от 30 до 15902. Их диаметры и значения λ, вычисленные численно, приведены в диссертации.

Опишем еще одно семейство графов Рамануджана — графы Пайзера. Их также называют графами изогений суперсингулярных эллиптических кривых. Такие графы находят интересные и многообещающие применения в постквантовой криптографии.

Как известно, эллиптической кривой над полем $\mathbb{F}$ называется гладкая алгебраическая кривая над этим полем, задаваемая уравнением вида $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, вместе с точкой в бесконечности O.

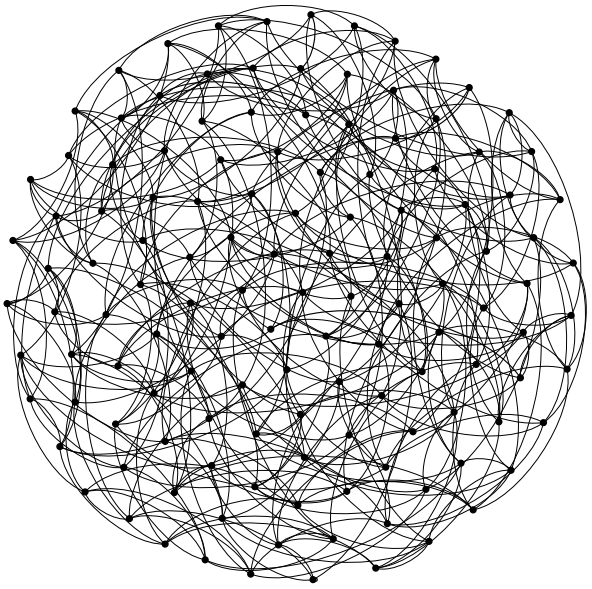

Рис. 1. Граф Пайзера $d = 6; N = 129$

Пусть p и l — простые числа, причем $p \equiv 1 \pmod{12}$, а l является квадратичным вычетом по модулю p. Множеством вершин графа Пайзера является множество классов изоморфизма суперсингулярных эллиптических кривых над полем $\mathbb{F}_{p^2}$. Вершины такого графа удобно задавать с помощью j-инвариантов соответствующих эллиптических кривых: будем писать «вершина j», имея в виду вершину, соответствующую классу изоморфизма эллиптических кривых с j-инвариантом j. Представителя такого класса будем обозначать как E_j.

Вершины j_1 и j_2 являются смежными, если существует l-изогения между

E_{j_1} и E_{j_2}. По определению, если E' и E'' — эллиптические кривые, то изогенией из E' в E'' называется морфизм $\varphi : E' \to E''$, для которого выполняется $\varphi(O) = O$. Изогения индуцирует гомоморфизм групп точек эллиптических кривых. Степенью изогении называется мощность ее ядра (в алгебраическом замыкании базового поля). Изогению степени l часто называют l-изогенией.

Построенный таким образом граф Пайзера $\Pi_{l,p}$, имеет $\lfloor \frac{p}{12} \rfloor$ вершин, является недвудольным $(l+1)$-регулярным графом и графом Рамануджана. Пример такого графа приведен на Рис. 1.

Небольших графов Пайзера существует достаточно много. Так, количество графов Пайзера степени 6 с числом вершин в диапазоне от 100 до 10000 составляет 1360. Некоторые графы Пайзера (степеней 4, 6, 8) были явно построены с целью проведения вычислительных экспериментов. Всего было построено 56 графов степени 6, 57 графов степени 4 и 21 граф степени 8. ПО для их построения разработано автором для системы компьютерной алгебры Magma. Диаметры и значения λ этих графов вычислены численно.

Далее в главе приводится алгоритм, позволяющий уменьшить число петель и кратных ребер в графе так, чтобы граф оставался регулярным. Для большинства сгенерированных в рамках настоящей работы графов его применение не приводило к существенному изменению параметра λ.

Проведены вычислительные эксперименты, которые подтвердили, что использование графов Рамануджана позволяет обеспечить хорошие характеристики лавинного эффекта, причем используемое семейство графов Рамануджана не оказывает существенного влияния на эти характеристики.

Нумерация ребер графа ОКлА. Будем называть *t-шаговой коллизией веса w* такие два различных заполнения ОКлА $x_1, x_2 \in \{0,1\}^N$, что $|x_1 \oplus x_2| = w$ и $F_A(x_1, t) = F_A(x_2, t)$, но $F_A(x_1, t-1) \neq F_A(x_2, t-1)$, где $|x|$ — вес вектора x. Заметим, что любая t-шаговая коллизия одновременно является и $(t+\tau)$-шаговой коллизией, для любого $\tau \in \mathbb{N}$.

Важны методы синтеза ОКлА, для которых коллизии или отсутствуют, или их нахождение является вычислительно трудной задачей. Будем называть такие ОКлА устойчивыми к коллизиям. В диссертации изучена устойчивость ОКлА к одношаговым коллизиям веса 1. Доказана следующая теорема.

Теорема 2. *Для обеспечения устойчивости однородного неориентированного ОКлА к одношаговым коллизиям веса 1 достаточно, чтобы ЛФС линейно зависела от одного из своих аргументов, а соответствующие этим аргументам ребра графа ОКлА порождали 2-фактор.*

Отметим, что в обсуждаемом случае связность 2-фактора не требуется и он может быть найден с помощью известного эффективного алгоритма. Найдя произвольный 2-фактор, следует для каждой его связной компоненты, являющейся циклом, сопоставить каждому ребру номер k относительно следующей в цикле вершины, где k — номер переменной, от которой ЛФС зависит линейно.

Третья глава начинается с построения семейства алгоритмов поточного шифрования, основанных на ОКлА. Далее разрабатывается метод построения псевдослучайных функций-кандидатов, основанных на ОКлА. На базе этих функций производится построение семейства алгоритмов блочного шифрования, двух семейств криптографических хэш-функций и семейства алгоритмов выработки имитовставки. Построенные в этой главе алгоритмы поточного и блочного шифрования предназначены для защиты компьютерных сетей от угроз нарушения конфиденциальности обрабатываемых в них данных, а хэш-функции и алгоритмы выработки имитовставки — для защиты компьютерных сетей от угроз нарушения целостности обрабатываемых в них данных, а также для применения в задачах обеспечения надежности и организации контроля передачи данных в компьютерных сетях. Все построенные алгоритмы предназначены для аппаратной реализации.

Заметим, что поскольку построенные симметричные криптографические алгоритмы задаются рядом параметров, в том числе графом и ЛФС ОКлА (одного или двух), различными константами, числом шагов (а для блочных шифров — и числом раундов) и др., мы говорим о семействах симметричных криптографических алгоритмов.

Построение алгоритмов поточного шифрования. Для построения алгоритма поточного шифрования используется идея объединения двух клеточных автоматов, впервые предложенная Б.М. Сухининым для построения генератора псевдослучайных двоичных последовательностей.

Итак, алгоритм поточного шифрования (назовем построенное в диссертации их семейство GRACE–S) представляет собой генератор гаммы, выход которого обычным образом накладывается на открытый текст. Генератор состоит из двух неориентированных однородных ОКлА с задающей последовательностью (обозначим их CA_1, CA_2) и LFSR. ОКлА имеют разный размер и различные ЛФС: f_1 и f_2. Задающая ячейка каждого из этих ОКлА выбирается в соответствии с результатами главы 2, а задающей последовательностью обоих ОКлА является выходная последовательность LFSR (его многочлен обратной связи должен быть примитивным). При этом число выходных ячеек обоих ОКлА должно быть одинаковым. Схема генератора гаммы показана на Рис. 2.

Начальным заполнением каждого ОКлА является ключ key, конкатенированный с некоторой константой, дополняющей его до размера ОКлА. Ключ является также начальным заполнением LFSR. Ключ не может состоять из одних нулей. Шифрование производится путем поразрядного сложения открытого текста с гаммой по модулю два. Расшифрование производится аналогично. При этом, для того чтобы обеспечить необходимые криптографические свойства ОКлА CA_1 и CA_2, их построение должно производиться в соответствии с результатами главы 2.

Обозначим заполнение ОКлА CA на шаге t, как $CA(t, M_0, \xi)$, где M_0 — начальное заполнение, а ξ — задающая последовательность. Выход ОКлА

обозначим $pr_m(CA(t, M_0, \xi))$, где m — длина выхода, а pr_m — функция, возвращающая некоторые m разрядов аргумента (имеющие наперед заданные номера). Последовательность ξ вырабатывается LFSR с начальным заполнением key. Выход генератора гаммы на шаге t вычисляется по формуле:

$$y(key, t) = pr_m(CA_1(t, key||c_1, \xi)) \oplus pr_m(CA_2(t, key||c_2, \xi)), \qquad (10)$$

где c_1 и c_2 — константы, дополняющие ключ до размера ОКлА, вес которых должен быть близок к половине длины; $||$ — операция конкатенации.

Вырабатываемая генератором гамма представляет собой конкатенацию выходов после определенного числа (τ) холостых шагов: $\gamma = y(key, \tau + 1)||y(key, \tau + 2)|| \ldots$.

Число τ должно быть больше диаметра графа. Поэтому, в случае использования графов Рамануджана, $\tau = \Omega(\log N)$, где N — размер большего ОКлА. Эмпирически обосновано, что на практике τ должно быть не меньше, чем $2D$, где D — диаметр графа ОКлА.

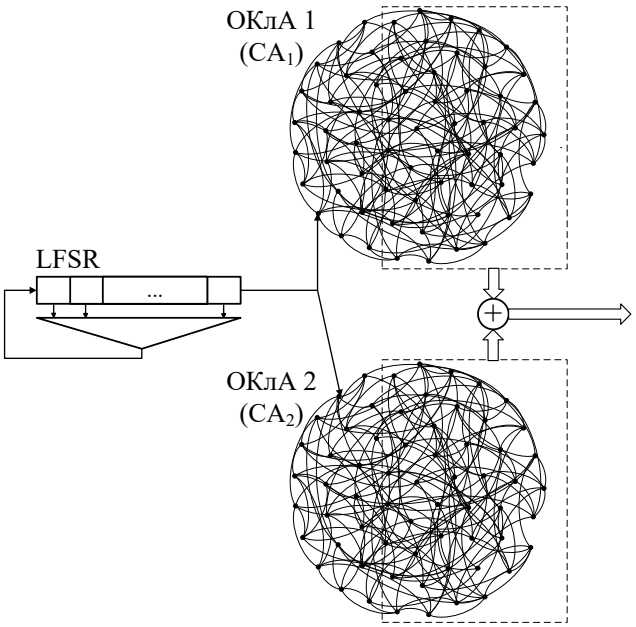

Рис. 2. Схема алгоритма поточного шифрования GRACE–S

Псевдослучайные функции. Понятие псевдослучайной функции — одно из основных в современной теоретической криптографии. Существуют теоретические подходы к определению псевдослучайной функции, которые, однако, нельзя использовать на практике. В то же время, на практике широко используются функции, которые не удается отличить от случайных с помощью известных методов. Поэтому, в данной работе мы удовлетворимся ослабленным определением псевдослучайности и будем называть псевдослучайными функциями-кандидатами функции вида $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$, которые невозможно отличить от случайных с помощью стандартного набора статистических тестов.

В диссертации предложено семейство псевдослучайных функций-кандидатов, основанных на ОКлА. Пусть требуется построить псевдослучайную функцию-кандидат $S : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$. Рассмотрим неориентированный однородный ОКлА A, содержащий $k+n+s$ ячеек, где s — некоторая величина, зависящая от n, которую будем называть числом скрытых вершин ОКлА. Построим псевдослучайную функцию-кандидат следующим образом:

$$S^A_{t,c,m}(key, x) = pr_m(F_A(x \parallel key \parallel c, t)), \qquad (11)$$

где $x \parallel y$ — конкатенация x и y; t — число шагов ОКлА; $c \in \{0,1\}^t$ — некоторая константа, вес которой приблизительно равен половине длины.

Число шагов t ОКлА и число скрытых вершин s выбирается так, чтобы функцию нельзя было отличить от случайной при помощи статистических тестов. Ясно, что для того, чтобы каждый разряд выхода функции зависел от всех разрядов входа, необходимо, чтобы выполнялось неравенство $t \geqslant D$, где D — диаметр графа. Для того чтобы функция проходила статистические тесты обычно требуется несколько большее число шагов.

Построение алгоритмов блочного шифрования. Для построения алгоритма блочного шифрования (назовем построенное в диссертации их семейство GRACE–B) определим следующее, основанное на схеме Фейстеля, раундовое преобразование:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus S^A_{t,c_i,m}(key_i, R_{i-1}), \end{aligned} \tag{12}$$

где i — номер раунда; m — длина блока; L_0, R_0 — левая и правая половины блока открытого текста; L_i, R_i — левая и правая половины блока после i-го раунда; key_i — раундовый ключ; A — неориентированный однородный ОКлА; t — число шагов ОКлА; c_i — раундовая константа.

При расшифровании выполняется преобразование, обратное преобразованию (12).

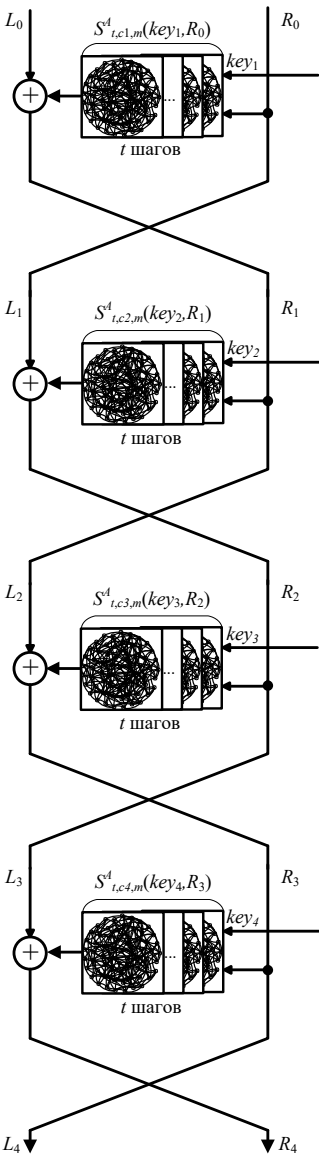

Рис. 3. Общая схема алгоритма блочного шифрования GRACE–B

Как обычно, алгоритм блочного шифрования состоит из нескольких раундов. Как следует из теоремы Любы–Ракоффа, число раундов должно быть не меньшим трех. Из соображений удобства можно рекомендовать четное число раундов. По-видимому, обычно хватает четырех раундов (общая схема для четырех раундов показана на Рис. 3). В конструкции алгоритма используется классическая схема Фейстеля, т.к. анализ показал, что использование обобщенных схем Фейстеля, в которых блок делится на три или более частей, нерационально и приводит к ухудшению производительности.

Построение криптографических хэш-функций и алгоритмов выработки имитовставки. Сформируем криптографическую хэш-функцию следующим образом. Разобьем сообщение X на блоки длины n: $X = (X_1, X_2, \ldots, X_q)$ (если длина сообщения не кратна длине блока, дополним его до длины блока тем или иным способом). Хэш, имеющий длину m, будем вычислять по формуле:

$$H(X) = S^A_{t_2,c_2,m}\left(c_3, \bigoplus_{i=1}^{q} S^A_{t_1,c_1,m_2}(i, X_i)\right), \tag{13}$$

где $c_1, c_2 \in \{0,1\}^s$ — различные константы, вес которых близок к $[s/2]$; $c_3 \in \{0,1\}^k$ — константа, вес которой близок к $[k/2]$; A — неориентированный однородный ОКлА; t_1, t_2 — числа шагов ОКлА; s — число скрытых ячеек ОКлА. ОКлА A должен иметь граф, построенный в соответствии с результатами главы 2. Должны выполняться условия $s \geqslant \frac{n+k}{2}$ и $m_2 \geqslant m$. Значение k следует выбирать так, чтобы максимальный номер блока помещался в k разрядов (например, $k = 64$). Параметры должны выбираться в соответствии с результатами главы 2.

Такая схема является вариантом древовидной схемы. Отметим, что выражением (13) задано семейство хэш-функций (будем его называть GRACE–H1). Достоинством этого семейства хэш-функций является возможность параллельного вычисления функции $S^A_{t_1,c_1,m}$ от разных блоков, что позволяет получить высокую производительность аппаратной реализации.

Другое семейство хэш-функций (назовем его GRACE–H2) использует схему, имеющую общие черты со схемой криптографической губки (Sponge). Принцип работы заключается в том, чтобы через определенное количество шагов неориентированного однородного ОКлА подмешивать к его заполнению очередной блок хэшируемого сообщения, а затем, опять-таки через определенное число шагов, снимать выходное значение. Опишем этот процесс более строго. Пусть n – длина блока хэш-функции. Разделим набор ячеек ОКлА на два набора, один — длины n, а другой — длины $(N - n)$. Будем записывать преобразование, выполняемое за t шагов ОКлА, в виде: $(x_{i+1}||y_{i+1}) = F_A(x_i||y_i, t)$. Тогда процесс вычисления хэш-функции состоит из трех этапов:

1. Этап абсорбирования: $(x_i||y_i) = F_A((x_{i-1} \oplus X_i)||y_{i-1}, t_1), \quad i = 1, 2, \ldots, q$;
2. Этап дополнительного перемешивания: $(h_1||z_1) = F_A(x_q||y_q, t_2)$;
3. Этап выжимания: $(h_{j+1}||z_{j+1}) = F_A(h_j||z_j, t_3)$.

При этом значением хэш-функции является конечная последовательность $h_1, h_2, \ldots, h_{\lceil s/n \rceil}$, необходимой длины.

В диссертации обосновано, что на основе ОКлА с достаточно большим числом ячеек можно строить функции формирования ключа (Key Derivation Function) — такие функции предназначены для формирования ключевой информации, а также для ряда других приложений.

Перейдем теперь к алгоритмам выработки имитовставки (MAC). Разработанные в диссертации алгоритмы выработки имитовставки (будем называть их семейство GRACE–MAC) состоят из двух этапов: этапа абсорбирования и этапа вычисления результата. На этапе абсорбирования будем использовать неориентированный однородный ОКлА, к заполнению которого раз в t_1 шагов (для некоторого t_1) подмешивается очередной блок сообщения. При этом, начальным заполнением ОКлА является ключ, с которым конкатенирована некоторая константа: $key||c_1$. Для обеспечения зависимости выхода от всех разрядов ключа используется задающая последовательность, вырабатываемая LFSR достаточной длины, характеристический многочлен

которого примитивен. В качестве начального заполнения LFSR используется ключ, конкатенированный с некоторой константой: $key||c_2$.

Обозначим преобразование, выполняемое ОКлА над его заполнением на одном шаге, как $G : \{0,1\}^N \to \{0,1\}^N$. Тогда заполнение ОКлА будет обновляться в соответствии с формулой:

$$(m_1(i), m_2(i), \ldots, m_N(i)) =$$
$$= \begin{cases} G(m_1(i-1), \ldots, m_{r-1}(i-1), m_r(i-1) \oplus \xi_i, \\ , m_{r+1}(i-1), \ldots, m_N(i-1)), & \text{если } i \neq 0 \pmod{t_1}; \\ G(m_1(i-1), \ldots, m_{\mu-1}(i-1), \\ , m_\mu(i-1) \oplus M_{\left(\frac{i}{t_1}-1\right)n+1}, \ldots, m_{\mu+n-1}(i-1) \oplus \\ \oplus M_{\left(\frac{i}{t_1}-1\right)n+n}, m_{\mu+n}(i-1), \ldots, m_{r-1}(i-1), \\ , m_r(i-1) \oplus \xi_i, m_{r+1}(i-1), \ldots, m_N(i-1)), & \text{если } i = 0 \pmod{t_1}. \end{cases}$$

Здесь: M_j — j-й разряд сообщения; n — длина блока сообщения; $\mu, \mu+1, \ldots, \mu+n-1$ — номера ячеек ОКлА, к которым подмешиваются разряды сообщения; $\{\xi_i\}$ — выходная последовательность LFSR, элементы которой прибавляются к ячейке m_r. Параметр r выбирается так, чтобы $r \notin \{\mu, \mu+1, \ldots, \mu+n-1\}$.

После того, как все сообщение будет обработано, этап абсорбирования завершается. Далее начинается этап вычисления результата, на котором ОКлА продолжает работать, при этом каждые t_2 шагов с некоторых разрядов его заполнения (например, разрядов с индексами $\mu \ldots, \mu+n-1$) снимаются двоичные разряды имитовставки. После того, как будет снято необходимое их количество, работа алгоритма завершается.

В диссертации подробно обоснован выбор параметров алгоритмов из разработанных семейств.

Глава 4 посвящена статистическому тестированию разработанных алгоритмов. Случайные и псевдослучайные последовательности, генераторы псевдослучайных последовательностей, псевдослучайные подстановки — важнейшие понятия, на которых базируется почти вся современная криптография. В связи с этим вопросы тестирования различных объектов на случайность являются очень важными. На практике под тестированием на случайность понимают статистическое тестирование. Оно является одним из важнейших этапов анализа любых симметричных криптоалгоритмов.

Глава начинается с краткого обзора подходов к определению понятия случайной последовательности и обзора наборов статистических тестов, в том числе DieHard, NIST Statistical Test Suite (NIST STS), RaBiGeTe и др. Наиболее исследованным и апробированным из них является NIST STS.

Далее в главе приводится обзор методик статистического тестирования блочных шифров. Наиболее распространенный подход к статистическому тестированию блочных шифров заключается в генерации различными спосо-

бами, посредством тестируемого шифра, псевдослучайных последовательностей, которые подвергаются тестированию с помощью какого-либо набора статистических тестов.

Рассматривается методика статистического тестирования блочных шифров NIST и ряд других. На основе методики NIST в диссертации разработана методика статистического тестирования псевдослучайных функций-кандидатов $S^A_{t,c,m}(key, x)$, семейство которых предложено в главе 3. С помощью этой методики протестированы эти функции с различными параметрами. В качестве графов их ОКлА использовались графы Пайзера, графы LPS-Y и случайные графы Рамануджана. В каждом случае проведено большое число тестов для различных размеров ОКлА (от 64 до 4100) и для различных длин блока и ключа. Во всех случаях, начиная с определенного числа шагов, функции успешно прошли все тесты, причем это число шагов не более чем 1.5 раза превышает диаметр графа и практически не зависит от используемого семейства графов Рамануджана.

Далее проводится статистическое тестирование алгоритмов блочного шифрования GRACE–B посредством методики NIST. Были протестированы 10 алгоритмов из этого семейства с длиной блока 128 бит, длиной ключа 128 и 256 бит, с четырьмя раундами, по 7 шагов на каждом раунде. При этом использовались графы LPS-Y, графы Пайзера и случайные графы Рамануджана. Все эти алгоритмы успешно прошли все статистические тесты.

Далее проводится статистическое тестирование алгоритмов поточного шифрования из семейства GRACE–S. Были протестированы эти алгоритмы с различными параметрами. Всеми протестированными алгоритмами были успешно пройдены все статистические тесты набора NIST STS.

Статистическое тестирование хэш-функций и алгоритмов выработки имитовставки проводилось с помощью набора статистических тестов NIST STS с помощью методики, которая приведена в диссертации. Всего было протестировано 54 хэш-функции из семейства GRACE–H2 (с различными наборами параметров) и столько же алгоритмов выработки имитовставки. Все протестированные алгоритмы успешно прошли статистические тесты. Что касается хэш-функций из семейства GRACE–H1, их хорошие статистические свойства следуют из хороших статистических свойств функций $S^A_{t,c,m}(key, x)$.

Таким образом, предположение о хороших статистических свойствах разработанных криптографических алгоритмов полностью подтвердилось.

Глава 5 посвящена исследованию криптостойкости разработанных алгоритмов. Криптостойкость, т.е. способность противостоять криптоанализу, является важнейшей характеристикой криптоалгоритмов.

NP-трудность задачи о восстановлении предыдущего состояния ОКлА. Пусть дан ОКлА и его заполнение после первого шага $M(1)$. Задачу нахождения такого начального заполнения ОКлА $M(0)$, которое после первого шага перейдет в $M(1)$, назовем *задачей о восстановлении предыдущего состояния ОКлА*. Сформулируем теперь эту задачу в форме распо-

знавания. Назовем *задачей о существовании предыдущего состояния ОКлА* задачу определения существования начального заполнения $M(0)$ ОКлА, которое после первого шага перейдет в $M(1)$. В диссертации доказана следующая теорема.

Теорема 3. *Задача о существовании предыдущего состояния однородного ОКлА является NP-полной.*

Из этой теоремы следует NP-трудность задачи о восстановлении предыдущего состояния ОКлА.

Исследование стойкости алгоритмов блочного шифрования, основанных на ОКлА, к линейному криптоанализу. Линейный криптоанализ является одним из наиболее известных методов криптоанализа блочных шифров. Он основан на использовании линейных приближений к описывающим работу шифра уравнениям. В диссертации доказано, что для того, чтобы алгоритм блочного шифрования, основанный на неориентированном однородном ОКлА с m-эластичной ЛФС, нелинейность которой удовлетворяет неравенству $\Lambda \geqslant 2^{d-1} - 2^{\lfloor \frac{d}{2} \rfloor}$, был стоек к линейному криптоанализу, достаточно, чтобы выполнялось хотя бы одно из условий (14), (15):

$$(m+1)(r-1)(t-2) + r - 1 \geqslant \frac{\|key\| - \|key_r\| - 2}{2\left\lceil \frac{d}{2} \right\rceil - 2}, \tag{14}$$

$$(m+1)(r-1)(t-2) + r - 1 > \frac{b-2}{2\left\lceil \frac{d}{2} \right\rceil - 2}, \tag{15}$$

а также, условие

$$(m+1)r(t-2) + r > \frac{b-2}{2\left\lceil \frac{d}{2} \right\rceil - 2}, \tag{16}$$

где $\|key\|$ — длина ключа шифра, $\|key_r\|$ — длина ключа последнего раунда, b — длина блока, m — порядок эластичности ЛФС.

Например, при $d = 6$, $b = 128$, $r = 4$, $m = 1$ (в качестве ЛФС используется функция (6)), $\|key\| = 256$, $\|key_r\| = 128$, получаем, что должно выполняться $t \geqslant 7$.

О применимости дифференциального криптоанализа. Дифференциальный (разностный) криптоанализ является одним из основных видов криптоанализа. Он основан на анализе влияния разностей между входными значениями на разности между выходными значениями. Проанализирована применимость классического дифференциального криптоанализа к разработанным алгоритмам блочного шифрования (GRACE–B) и сделан вывод, что он к этим алгоритмам напрямую неприменим.

Исследование стойкости к алгебраическому криптоанализу. Проведено эмпирическое исследование стойкости основанных на ОКлА криптоалгоритмов по отношению к алгебраическому криптоанализу, основанному на применении базисов Грёбнера для решения системы полиномиальных уравнений, описывающей шифр. Для построения базисов Грёбнера в диссертации используется алгоритм Фужера F4, реализованный в библиотеке

Polybori и в системе компьютерной алгебры Magma.

Криптоанализ шифров и хэш-функций, основанных на ОКлА, может сводиться к различным задачам. Здесь мы будем рассматривать задачу, которую назовем задачей восстановления ключа ОКлА. Сформулируем ее следующим образом. Дан ОКлА, натуральное число s, начальные значения некоторых ячеек и значения некоторых ячеек после s шагов этого ОКлА. Требуется найти начальные значения остальных ячеек (их количество будем называть *длиной ключа*). Если найдется алгоритм решения этой задачи, работающий быстрее, чем полный перебор всех наборов неизвестных начальных значений, то криптоалгоритмы, основанные на ОКлА, могут оказаться нестойкими.

Очевидно, что, k шагов ОКлА, имеющего N ячеек, описываются системой из kN уравнений, каждое из которых имеет вид (1). Если к этой системе уравнений добавить уравнения, соответствующие известным начальным и конечным значениям ячеек, то ее решение является решением задачи восстановления ключа ОКлА.

Для обоснования стойкости криптоалгоритмов, основанных на ОКлА, к алгебраическому криптоанализу, был проведен вычислительный эксперимент по решению задачи восстановления ключа ОКлА. Цель эксперимента состояла в определении максимального размера ОКлА, для которого ее решение возможно на практике. С помощью разработанной автором программы генерировались случайные 6-регулярные графы Рамануджана с необходимым числом вершин. Во всех вычислительных экспериментах длина ключа полагалась равной $\lfloor \frac{N}{2} \rfloor$. Для каждого графа генерировалась система уравнений, описывающая k шагов соответствующего неориентированного однородного ОКлА. При этом в качестве ЛФС использовалась функция (6). Полученные системы решались как с помощью системы Magma v2.21-5, так и с помощью библиотеки Polybori 0.8.3 на компьютере с 16-ю ядрами Intel Xeon E5-2690 и 16 ГБ ОЗУ, работающем под управлением OS Linux.

Библиотека Polybori показала гораздо лучшую производительность по сравнению с системой Magma. Но решить задачу восстановления ключа ОКлА с помощью Polybori оказалось практически возможным лишь для малых значений числа ячеек (14–20, в зависимости от числа шагов), что обуславливается очень быстрым ростом требований к памяти. При этом время работы существенно (на несколько порядков) превышает время полного перебора на ПЛИС, а зависимость времени работы от числа ячеек имеет экспоненциальный характер. Это подтверждает, что алгебраический криптоанализ блочных шифров и хэш-функций, основанных на ОКлА с числом ячеек, использующимся на практике (порядка нескольких сотен и более), с помощью существующих средств, основанных на применении базисов Грёбнера, невозможен.

Исследование стойкости к логическому криптоанализу. Логический криптоанализ основан на представлении криптографического преобразования в виде конъюнктивной нормальной формы с последующим решением

задачи КНФ-выполнимости (SAT) посредством предназначенных для ее решения алгоритмов — так называемых SAT-решателей.

В диссертации эмпирически продемонстрировано, что с помощью существующих SAT-решателей невозможно решить задачу восстановления ключа ОКлА быстрее, чем полным перебором. Заметим, что решать эту задачу для ОКлА используемого на практике размера практически невозможно, в связи с огромной вычислительной сложностью. Поэтому в диссертации вычислительные эксперименты по решению этой задачи проводились для ОКлА малого размера.

Пусть известны начальные значения ячеек с номерами $u_1, u_2, \ldots, u_{n_{left}}$: $\alpha_{u_1}, \alpha_{u_2}, \ldots, \alpha_{u_{n_{left}}}$ и конечные значения ячеек с номерами $v_1, v_2, \ldots, v_{n_{right}}$: $\beta_{v_1}, \beta_{v_2}, \ldots, \beta_{v_{n_{right}}}$ (конечными будем называть значения ячеек после s шагов ОКлА). Пусть $\mathcal{F}(z_1, \ldots z_d, y)$ — КНФ, которая равна 1 тогда и только тогда, когда выполняется равенство $y = f(z_1, \ldots, z_d)$, где f — ЛФС. Тогда s шагам ОКлА соответствует КНФ:

$$\left(\bigwedge_{j=1}^{n_{left}} x_{u_j}^{\alpha_{u_j}}\right) \wedge \left(\bigwedge_{j=1}^{n_{right}} x_{u_j+sN}^{\beta_{v_j}}\right) \wedge$$
$$\wedge \left(\bigwedge_{k=0}^{s-1} \bigwedge_{i=1}^{N} \mathcal{F}(x_{\eta(i,1)+kN}, x_{\eta(i,2)+kN}, \ldots, x_{\eta(i,d)+kN}, x_{i+(k+1)N})\right), \tag{17}$$

где, как обычно, $x^\sigma = x$, если $\sigma = 1$, и $x^\sigma = \overline{x}$, если $\sigma = 0$, а переменная x_{i+jN} соответствует значению i-й ячейки на шаге j.

Набор, на котором КНФ (17) равна единице, содержит решение задачи восстановления ключа ОКлА.

Для проведения вычислительных экспериментов в диссертации используются конкретные параметры. Так, в качестве графов ОКлА выбраны 6-регулярные графы Пайзера. В качестве ЛФС используется функция (6). Кроме того, полагаются известными начальные значения ячеек с номерами $1, 2, \ldots, \lfloor N/2 \rfloor$ и конечные значения этих же ячеек. Значения остальных ячеек считаются неизвестными. Необходимо найти начальные значения ячеек с номерами $\lfloor N/2 \rfloor + 1, \lfloor N/2 \rfloor + 2, \ldots, N$ (то есть, длина ключа составляет $\lceil N/2 \rceil$ ячеек).

Итак, необходимо найти набор, на котором функция, заданная формулой (17), равна единице. Отметим, что очевидным способом решения этой задачи является перебор, объем которого составляет $2^{\lceil N/2 \rceil}$ итераций. Мы же будем использовать SAT-решатель. В настоящее время существует большое число SAT-решателей. Поскольку для разных задач могут лучше подходить различные SAT-решатели, в диссертации проведено эмпирическое сравнение следующих SAT-решателей: PicoSat 965, MiniSat 2.2, Glucose 4.1, Lingeling, CryptoMiniSat 5, которые выполнялись на компьютере с 16-ю ядрами Intel Xeon E5-2609 и 10 ГБ ОЗУ, под управлением ОС Linux. Программа, генерирующая КНФ вида (17), написана автором на языке программирования

Python. Лучшее время показал MiniSat, из чего можно заключить, что для решения данной задачи он подходит лучше всего. Он и использовался в дальнейших вычислительных экспериментах.

Проведены замеры времени, требуемого для решения посредством SAT-решателя MiniSat задачи восстановления ключа ОКлА, графы которых являются графами Пайзера степени 6 с различным числом вершин (длина ключа при этом равна $\lceil N/2 \rceil$, где N — число вершин графа), для различного числа шагов ОКлА ($6, 8, 10, 12$ и 14). Сравнение со временем, необходимым для решения этой же задачи методом полного перебора с использованием ПЛИС, показало, что решение с помощью SAT-решателя потребовало гораздо (на несколько порядков) больше времени, чем полный перебор, а эмпирические зависимости времени работы SAT-решателя от размера ОКлА (и от длины ключа) имеют экспоненциальный характер.

О стойкости к квантовому криптоанализу. В диссертации проанализирована применимость квантового криптоанализа к основанным на ОКлА криптоалгоритмам. Проведенный анализ показал, что на основе ОКлА возможно построить алгоритмы шифрования, которые требует достаточно много квантовой памяти для реализации на квантовом компьютере (например, десятки или сотни тысяч кубитов). Можно предположить, что, когда практические квантовые компьютеры появятся, размер их квантовой памяти будет небольшим и с их помощью нельзя будет взломать такой шифр.

Таким образом, проведенные исследования показали высокий уровень криптостойкости разработанных криптоалгоритмов.

Глава 6 посвящена реализации разработанных алгоритмов и тестированию их производительности. Прежде всего рассматривается аппаратная реализация разработанных алгоритмов на ПЛИС, с целью подтверждения высокой производительности. Кроме того, рассматривается возможность реализации разработанных алгоритмов на графических процессорах.

Реализация на ПЛИС. ПЛИС — это интегральная микросхема, логика работы которой задается посредством программирования. С помощью ПЛИС можно реализовать практически любую цифровую схему. В настоящей работе в качестве платформы были выбраны ПЛИС фирмы Altera, а в качестве языка описания — VHDL.

Основой архитектуры ПЛИС Altera являются модули адаптивной логики (Adaptive Logic Module, ALM). Каждый ALM состоит из элемента комбинаторной логики, двух регистров и двух сумматоров. С помощью элемента комбинаторной логики можно реализовать булеву функцию. Причем младшие модели ПЛИС Altera (семейство Cyclone) позволяют реализовать в каждом ALM произвольную булеву функцию от четырех переменных, а старшие модели (семейства Arria и Stratix) — от шести переменных. Поэтому для обеспечения высокой эффективности, ЛФС ОКлА должна зависеть не более чем от шести переменных и должна допускать возможность реализации с помощью как можно меньшего числа функций, зависящих от четырех переменных. В

диссертации показано, что построенное в главе 2 семейство ЛФС удовлетворяет этим требованиям. Например, шестиместная ЛФС данного вида может быть представлена в виде суперпозиции двух четырехместных функций.

Разработан комплекс программ, позволяющий генерировать VHDL-файлы, описывающие схемы, реализующие основанные на ОКлА криптоалгоритмы, заданные параметрами, такими как графы ОКлА, ЛФС и др. Комплекс программ реализован на языке C#. Для компиляции VHDL-файлов и моделирования использовались САПР Altera Quartus II 12.0 и Altera ModelSim.

Было проведено исследование производительности при различных наборах параметров, на различных ПЛИС фирмы Altera (Cyclone II, Cyclone V, Arria II GX, Arria V, Stratix III, Stratix V). Для ПЛИС Cyclone II и Stratix V была проверена работа на физической ПЛИС, с помощью соответствующих отладочных плат с внешним тактовым генератором.

Сравнение производительности семейства криптоалгоритмов GRACE–S проводилось с поточными шифрами, представленными на европейский конкурс алгоритмов поточного шифрования eSTREAM: Grain, Achterbahn, Trivium, MICKEY, MOSQUITO, SFINKS+, VEST, а также с алгоритмом AES в режиме OFB. Сравнение эффективности и требований к аппаратным ресурсам проводилось с алгоритмами Grain, AES (в режиме OFB), Trivium, MICKEY. Причем сравнение производительности осуществлялось с реализациями этих алгоритмов, ориентированными на высокую производительность, а сравнение эффективности и требований к аппаратным ресурсам (ресурсоемкости) осуществлялось с реализациями, ориентированными на максимальную экономию аппаратных ресурсов. Ресурсоемкость в диссертации оценивается в LE — логических элементах (эквивалентных логических элементах), либо в ALUT (Adaptive Look-Up Table). Под эффективностью аппаратной реализации понимается отношение производительности к ресурсоемкости.

Результаты тестов производительности на ПЛИС Altera Stratix V приведены в Таблице 1. В соответствии с ними, для разработанных алгоритмов поточного шифрования из семейства GRACE–S, при определенных параметрах, была достигнута производительность, превышающая 1100 Гбит/с, что более чем в 50 раз превышает производительность лучшего по этому параметру алгоритма шифрования из тех, с которыми производилось сравнение (Trivium). Требования к аппаратным ресурсам составляли от 1 тыс. LE, что совпадало по порядку с требованиями других алгоритмов. Эффективность реализации достигала 179 Гбит/(с·LE), что более чем в 7 раз превышало эффективность лучшего по этому параметру из алгоритмов, с которыми проводилось сравнение (Trivium).

В диссертации приведены результаты измерения параметров реализации алгоритмов блочного шифрования из семейства GRACE–B на ПЛИС Altera. Было разработано две реализации — конвейерная, которая ориентирована на достижение максимальной производительности, но требует относительно много аппаратных ресурсов, и низкоресурсная — эффективно использующая ап-

Таблица 1.

Производительность алгоритмов поточного шифрования на ПЛИС

Алгоритм	Производительность при макс. тактовой частоте, Гбит/с	Производительность при тактовой частоте 100 МГц, Гбит/с
GRACE–S – 256	179	25
GRACE–S – 1024	529	102
GRACE–S – 3072	1112	307
AES (OFB)	0.52	0.29
Achterbahn	0.46	0.18
Grain	4.47	1.49
MICKEY	0.28	0.93
MOSQUITO	0.73	0.27
SFINKS+	1.24	0.74
Trivium	18.5	5.95
VEST	4.25	1.48

паратные ресурсы, однако обладающая меньшей производительностью. Для конвейерной реализации производительность алгоритмов блочного шифрования сравнивалась с производительностью алгоритма AES, являющегося государственным стандартом США. Для низкоресурсной реализации сравнение производилось с низкоресурсными реализациями алгоритма блочного шифрования AES для длины блока 128 бит и алгоритма блочного шифрования Present для длины блока 64 бита.

Для конвейерной реализации была достигнута производительность в 53 Гбит/с, что приблизительно в 2.5 раза превышает производительность лучших реализаций алгоритма AES при приблизительно таких же требованиях к аппаратным ресурсам. Для низкоресурсной реализации с длиной блока 64 достигнута производительность в 0.7 Гбит/с, что приблизительно в 3.5 раза больше, чем у алгоритма Present, а ресурсоемкость составила около 460 LE.

Таким образом, из представленных результатов видно, что алгоритмы блочного шифрования из разработанного семейства при конвейерной реализации на ПЛИС обладают значительно более высокой производительностью и, вместе с тем, лучшей эффективностью реализации, чем алгоритм AES. В то же время, при низкоресурсной реализации получается значительно более высокая производительность по сравнению с алгоритмами AES и Present при сопоставимой ресурсоемкости.

Рассмотрим теперь реализацию хэш-функций из семейства GRACE–H1. Максимальная производительность в 198 Гбит/с была достигнута на ПЛИС Altera Stratix V. Сравнение производительности проведено с хэш-функцией Keccak, являющейся стандартом США SHA-3, хэш-функциями BLAKE, Groestl, JH, Skein, которые являются финалистами конкурса NIST Hash Function Competition, а также хэш-функцией SHA-256, тоже являющейся

стандартом США. При этом сравнение производительности осуществлялось с реализацией для ПЛИС Stratix III (т.к. для этой ПЛИС в литературе представлено больше всего данных по производительности). На этой ПЛИС максимальная производительность хэш-функции семейства GRACE–H1 составила 165 Гбит/с. Это в 16 раз превышает производительность лучшей по этому параметру хэш-функции сравнения (SHA-3). По эффективности аппаратной реализации на ПЛИС Altera Stratix III некоторые хэш-функции из семейства GRACE–H1 приблизительно в 4 раза лучше, чем лучшая по этому параметру хэш-функция сравнения.

Рассмотрим теперь производительность хэш-функций из семейства GRACE–H2. Эти хэш-функции с различными длинами блока, на основе различных графов Пайзера, реализованы на языке VHDL для ПЛИС фирмы Altera. Для ПЛИС Stratix III производительность при определенных значениях параметров превышает 130 Гбит/с, что на порядок превышает производительность лучших реализаций хэш-функции SHA-3 при сопоставимой ресурсоемкости.

Реализация на GPU. Криптографические алгоритмы, основанные на ОКлА, могут быть реализованы не только аппаратно, но и программно — на графических процессорах (GPU). Современные GPU представляют собой вычислительные устройства, имеющие массивно параллельную архитектуру. ОКлА состоит из набора ячеек, над которыми производятся однотипные вычисления, что дает возможность эффективной реализации на GPU.

Для реализации поточных шифров, блочных шифров и хэш-функций на GPU в диссертации используется OpenCL, представляющий собой универсальный интерфейс для гетерогенных вычислений. Разработанный комплекс программ написан на языке C++ и позволяет пользователю устанавливать различные параметры.

При проведении тестирования использовалось GPU NVIDIA GTX 650, NVIDIA GTX 770, AMD R9 280X. Приведем здесь максимальную из скоростей, достигнутых на этих трех GPU (остальные данные приведены в диссертации). Для алгоритмов поточного шифрования GRACE–S получена производительность до 527 Мбит/с. Причем ввиду того, что продемонстрирована хорошая масштабируемость при увеличении числа потоков гаммы, предложено обобщение семейства алгоритмов, позволяющее достичь производительности до 6607 Мбит/с (в зависимости от числа потоков гаммы и размера ОКлА).

Для алгоритмов блочного шифрования GRACE–B при восьми шагах на раунд, производительность в режиме счетчика достигала 382 Мбит/с. Производительность в режиме ECB отличалась несущественно. Производительность в режиме CBC достигала 29 Мбит/с. Для хэш-функций GRACE–H1 производительность составила 2409 Мбит/с для девяти шагов. Достигнутый уровень производительности на GPU во всех случаях, кроме алгоритма блочного шифрования в режиме CBC, совпадает по порядку с уровнем производительности современных криптоалгоритмов, ориентированных на программ-

ную реализацию, при их реализации на CPU. Этот факт делает возможным применение разработанных криптоалгоритмов не только на ПЛИС и специализированных микросхемах, но и практически на любом современном вычислительном устройстве, имеющем графический ускоритель, в т. ч., на персональных компьютерах, ноутбуках, планшетных компьютерах и смартфонах.

В **Заключении** перечислены основные полученные в диссертации результаты, которые заключаются в следующем:

1. Исследованы методы построения расширяющих графов, подходящих для применения в криптоалгоритмах, основанных на ОКлА. Такими графами являются графы Рамануджана. Рассмотрены рандомизированный и детерминированный подходы к их построению. Разработано ПО для построения таких графов, с помощью которого построено большое количество графов и вычислены значения их параметров.
2. Исследованы вопросы построения ЛФС ОКлА. Выдвинуты и научно обоснованы требования к таким функциям. Построено семейство функций, доказуемо удовлетворяющих этим требованиям.
3. Исследованы вопросы нумерации ребер графа ОКлА. Предложен способ нумерации ребер, доказуемо обеспечивающий стойкость к коллизиям определенного вида.
4. Разработано семейство ориентированных на аппаратную реализацию алгоритмов поточного шифрования, основанных на ОКлА.
5. Разработан метод построения псевдослучайных функций-кандидатов, основанных на ОКлА.
6. Разработано семейство ориентированных на аппаратную реализацию алгоритмов блочного шифрования на основе построенных псевдослучайных функций-кандидатов.
7. Построены два семейства ориентированных на аппаратную реализацию криптографических хэш-функций, основанных на ОКлА и предложена концепция их использования в качестве функций формирования ключа.
8. Построено семейство основанных на ОКлА алгоритмов выработки имитовставки, ориентированных на аппаратную реализацию.
9. Проведено тестирование статистических свойств ОКлА и основанных на них криптоалгоритмов. Его результаты подтверждают высокое статистическое качество этих алгоритмов.
10. Доказана теорема о NP-трудности восстановления предыдущего состояния ОКлА.
11. Произведено теоретическое исследование стойкости построенных криптоалгоритмов по отношению к линейному криптоанализу. Получены условия, которым должны удовлетворять параметры для обеспечения криптостойкости.
12. Произведено эмпирическое исследование стойкости разработанных криптоалгоритмов по отношению к алгебраическому криптоанализу, основанному на построении базисов Грёбнера. Результаты исследования

подтверждают стойкость криптографических алгоритмов, основанных на ОКлА, к данному методу криптоанализа.

13. Произведено эмпирическое исследование стойкости построенных криптоалгоритмов по отношению к логическому криптоанализу, основанному на использовании SAT-решателей. Результаты исследования подтверждают стойкость разработанных криптографических алгоритмов к данному методу криптоанализа.
14. Исследована возможность применения дифференциального криптоанализа и квантового криптоанализа к разработанным криптоалгоритмам.
15. Произведена аппаратная реализация построенных криптографических алгоритмов (алгоритмов поточного шифрования, алгоритмов блочного шифрования, криптографических хэш-функций) на базе ПЛИС. Проведено тестирование полученных реализаций и их сравнение с лучшими реализациями существующих криптоалгоритмов аналогичного назначения. Показано, что производительность разработанных алгоритмов существенно превышает производительность лучших аналогов.
16. Алгоритмы блочного шифрования, поточного шифрования и хэширования, основанные на ОКлА, реализованы на графических процессорах. Протестирована производительность.

Комплекс полученных результатов представляет собой методологию синтеза симметричных криптоалгоритмов, основанных на ОКлА. Эта методология позволяет производить построение как высокопроизводительных, так и низкоресурсных симметричных криптографических алгоритмов, предназначенных для аппаратной реализации, в том числе алгоритмов поточного шифрования, алгоритмов блочного шифрования, криптографических хэш-функций и алгоритмов выработки имитовставки. Использование таких алгоритмов для защиты компьютерных сетей позволит повысить их пропускную способность.

ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

— Публикации в изданиях из перечня ВАК РФ —

1. Ключарёв П.Г. Детерминированные методы построения графов Рамануджана, предназначенных для применения в криптографических алгоритмах, основанных на обобщённых клеточных автоматах // Прикладная дискретная математика. 2018. № 42. С. 76–93. (Scopus) (1.1 п.л.)
2. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1(19). С. 45–50. (0.6 п.л.)
3. Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 1 // Вопросы кибербезопасности. 2021. № 6(46). С. 90–101. DOI: 10.21681/2311-3456-2021-6-90-101. (1.1 п.л.)
4. Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 2 // Вопросы кибербезопасности. 2022. № 1(47). С. 37–48.

DOI: 10.21681/2311-3456-2022-1-37-48. (1.2 п.л.)
5. Ключарёв П.Г. Клеточные автоматы, основанные на графах Рамануджана, в задачах генерации псевдослучайных последовательностей // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2011. № 10. Режим доступа: http://www.technomag.edu.ru/doc/241308.html. (0.9 п.л.)
6. Ключарёв П.Г. Исследование практической возможности решения связанных с криптоанализом задач на обобщенных клеточных автоматах алгебраическими методами // Математика и математическое моделирование. 2017. № 5. С. 29–44. DOI: 10.24108/mathm.0517.0000080. (1 п.л.)
7. Ключарёв П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. Режим доступа: http://technomag.edu.ru/doc/312834.html. (0.4 п.л.)
8. Ключарёв П.Г. Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 9. С. 194–202. Режим доступа: http://technomag.edu.ru/doc/727086.html. (0.5 п.л.)
9. Ключарёв П.Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. С. 214–223. Режим доступа: http://engineering-science.ru/doc/675812.html. (0.6 п.л.)
10. Ключарёв П.Г. О статистическом тестировании блочных шифров // Математика и математическое моделирование. 2018. № 5. С. 35–57. DOI: 10.24108/mathm.0518.0000132. (1.4 п.л.)
11. Ключарёв П.Г. Квантовый компьютер и криптографическая стойкость современных систем шифрования // Вестник МГТУ им. Н.Э. Баумана. Серия Естественные науки. 2007. № 2. С. 113–120. (0.7 п.л.)
12. Ключарёв П.Г. О периоде обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 2. Режим доступа: http://technomag.edu.ru/doc/340943.html. (0.3 п.л.)
13. Ключарёв П.Г. Обеспечение криптографических свойств обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 3. Режим доступа: http://technomag.edu.ru/doc/358973.html. (0.5 п.л.)
14. Ключарёв П.Г. О вычислительной сложности некоторых задач на обобщенных клеточных автоматах // Безопасность информационных технологий. 2012. № 1. С. 30–32. (0.2 п.л.)
15. Ключарёв П.Г. Построение псевдослучайных функций на основе обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 10. С. 263–274. DOI: 10.7463/1112.0496381. (0.7 п.л.)

16. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 12. С. 361–374. Режим доступа: http://engineering-science.ru/doc/517543.html. (0.8 п.л.)
17. Ключарёв П.Г. Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 1. С. 161–172. DOI: 10.7463/0113.0534640. (0.7 п.л.)
18. Ключарёв П.Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 10. С. 299–314. Режим доступа: http://engineering-science.ru/doc/624722.html. (1 п.л.)
19. Ключарев П.Г. Основы квантовых вычислений и квантовой криптографии // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия: Приборостроение. 2006. № 2. С. 36–46. (0.9 п.л.)
20. Ключарёв П.Г., Чесноков В.О. Исследование спектральных свойств социального графа сети LiveJournal // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 9. С. 391–400. Режим доступа: http://engineering-science.ru/doc/603441.html. (0.6 п.л./0.3 п.л.)
21. Ключарёв П.Г. Исследование стойкости блочных шифров, основанных на обобщенных клеточных автоматах, к линейному криптоанализу // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 5. С. 235–246. Режим доступа: http://engineering-science.ru/doc/574231.html. (0.7 п.л.)
22. Ключарёв П.Г. Производительность поточных шифров, основанных на клеточных автоматах, при реализации на графических процессорах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 6. С. 200–213. Режим доступа: http://engineering-science.ru/doc/842091.html. (0.8 п.л.)
23. Ключарёв П.Г. Производительность древовидных криптографических хэш-функций, основанных на клеточных автоматах, при их реализации на графических процессорах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 10. С. 132–142. Режим доступа: http://engineering-science.ru/doc/847891.html. (0.6 п.л.)
24. Ключарёв П.Г. Построение алгоритмов выработки имитовставок на основе обобщённых клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2016. № 11. С. 142–152. Режим доступа: http://engineering-science.ru/doc/849590.html. (0.6 п.л.)
25. Балк Е.А., Ключарёв П.Г. Исследование характеристик лавинного эффекта обобщенных клеточных автоматов на основе графов малого диаметра // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн.

2016. № 4. С. 92–105. Режим доступа: http://engineering-science.ru/doc/837506.html. (0.8 п.л./0.3 п.л.)

26. Ключарёв П.Г. Построение случайных графов, предназначенных для применения в криптографических алгоритмах, основанных на обобщенных клеточных автоматах // Математика и математическое моделирование. 2017. № 3. С. 77–90. Режим доступа: https://www.mathmelpub.ru/jour/article/view/76. (0.8 п.л.)
27. Ключарёв П.Г., Басараб М.А. Спектральные методы анализа социальных сетей // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2017. № 5. С. 168–177. Режим доступа: https://www.elibrary.ru/item.asp?id=30585833. (0.9 п.л./0.7 п.л.)
28. Анализ моделей трафика сетей передачи данных / А.М. Андреев, П.Г. Ключарёв, С.М. Джаммул, А.В. Бабиченко // Прикладная физика и математика. 2018. № 4. С. 42–51. (0.6 п.л./0.15 п.л.)

— Публикации в прочих рецензируемых журналах —

29. Ключарёв П.Г. Исследование практической возможности решения одной задачи на обобщенных клеточных автоматах с использованием SAT-решателей // Машиностроение и компьютерные технологии. 2018. № 11. С. 11–22. Режим доступа: https://www.elibrary.ru/item.asp?id=37315433. (0.7 п.л.)
30. Ключарёв П.Г. Криптоаналитические возможности квантового компьютера // Прикаспийский журнал: управление и высокие технологии. 2008. № 2. С. 7–13. (0.4 п.л.)
31. Ключарёв П.Г. О производительности блочных шифров, основанных на клеточных автоматах, при их реализации на графических процессорах // Радиооптика. 2016. № 6. С. 24–34. DOI: 10.7463/rdopt.0616.0850899. (0.6 п.л.)

— Публикации в тезисах конференций —

32. Ключарёв П.Г. Криптографические свойства клеточных автоматов, основанных на графах Любоцкого-Филипса-Сарнака // Безопасные информационные технологии. Сборник трудов Второй всероссийской научно-технической конференции. М.: НИИ радиоэлектроники и лазерной техники, 2011. С. 163–173. (0.7 п.л.)
33. Ключарёв П.Г. Построение клеточно-автоматных псевдослучайных функций // Безопасные информационные технологии. Третья всероссийская научно-техническая конференция. Сборник трудов. М.: НИИ Радиоэлектроники и лазерной техники, 2012. С. 82–87. (0.3 п.л.)
34. Ключарёв П.Г. О построении криптографических хэш-функций на базе обобщенных клеточных автоматов // Безопасные информационные технологии. Сборник трудов Четвертой всероссийской научно-технической конференции. М.: НИИ Радиоэлектроники и лазерной техники, 2013. С. 162–164. (0.1 п.л.)
35. Ключарёв П.Г. Теория расширяющих графов в структуре учебного пла-

на подготовки специалистов по специальности «Компьютерная безопасность» // Инновационные методы обучения в заочной системе образования. Межвузовская научная конференция. Сборник трудов. М.: ООО «Угрешская типография», 2013. С. 90–94. (0.3 п.л.)

36. Балк Е.А., Ключарёв П.Г. Исследование характеристик лавинного эффекта неориентированных обобщенных клеточных автоматов малого размера // Перспективы развития информационных технологий: сборник материалов XI международной научно-практической конференции. Новосибирск: Сибпринт, 2013. С. 7–13. (0.3 п.л./0.1 п.л.)
37. Ключарёв П.Г. Обобщённые клеточные автоматы, как основа для построения функций формирования ключа // Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции / М.: НУК Информатика и системы управления. 2016. С. 162–164. (0.1 п.л.)
38. Ключарёв П.Г. Об анализе блочных шифров, основанных на обобщенных клеточных автоматах // Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2017. С. 237–240. (0.2 п.л.)
39. Ключарёв П.Г. Квантовые вычисления и атаки на криптоалгоритмы, основанные на обобщенных клеточных автоматах // Безопасные информационные технологии. Сборник трудов Восьмой всероссийской научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2017. С. 234–236. (0.1 п.л.)
40. Ключарёв П.Г. О производительности и статистических свойствах некоторых криптографических алгоритмов, основанных на обобщенных клеточных автоматах // Безопасные информационные технологии. Сборник трудов Девятой всероссийской научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2018. С. 91–94. (0.1 п.л.)
41. Ключарёв П.Г. Графы Пайзера в задачах криптографии и обработки информации // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2019. С. 176–179. (0.2 п.л.)
42. Постквантовый криптографический протокол выработки общего ключа, основанный на изогениях суперсингулярных эллиптических кривых / С.В. Гребнев, П.Г. Ключарёв и др. // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2021. С. 99–103. (0.2 п.л./0.04 п.л.)
43. Ключарёв П.Г. О криптографических алгоритмах, основанных на обобщенных клеточных автоматах, и перспективах их применения // Безопасные информационные технологии. Сборник трудов XI международной научно-технической конференции. М.: МГТУ им. Н.Э. Баумана, 2021. С. 135–138. (0.2 п.л.)